# Manual da
# ***Due Diligence***

Manual de apoio para preenchimento de avaliações de continuidade de negócios, privacidade e segurança da informação.

ICATU

# CONTEÚDO

# Este manual

Este manual foi elaborado para ajudar empresas prestadoras de serviços ou fornecedores de produtos para o **Grupo Icatu** a concluir a etapa de *due diligence* da contratação.

**O que é uma *due diligence*?** É uma avaliação que o **Grupo Icatu** realiza para apurar se uma empresa segue o disposto na lei, em regulamentos específicos e/ou se possui processos, medidas e controles relacionados aos temas que são importantes para o **Grupo Icatu**. A *due diligence* se apresenta no formato de questionário, que é respondido na plataforma *online* **OneTrust**.

**A quem se destina?** A todas as pessoas físicas ou jurídicas, fornecedores de produtos ou prestadores de serviços **(Sua Empresa)** que tiverem interesse em ser contratados pelo **Grupo Icatu**.

**Por que ela é importante?** Porque permite que o **Grupo Icatu** conheça a **Empresa,** entendendo como ela contribui para a continuidade dos nossos negócios, como se posiciona em matéria de proteção de dados pessoais e como seu polo de tecnologia se desenvolve, a partir de regramentos técnicos para a garantia da segurança das informações.

ICATU

# Diretrizes de preenchimento

Conforme o quadro abaixo, é possível receber mais de um questionário.

| | Avaliaremos | Com o objetivo de | Importante observar |
|---|---|---|---|
| **Continuidade de Negócios** | Como **Sua Empresa** e seus produtos contribuem para a continuidade dos negócios do **Grupo Icatu** | Conhecer a maturidade de **Sua Empresa** no que tange à gestão de continuidade de negócios, ao cumprimento da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) e à verificação de requisitos mínimos e ações recomendadas para defesa cibernética | As diligências focarão em **Sua Empresa** como um todo não apenas o serviço para o qual **Você** a está cadastrando, nem o papel de **Sua Empresa** enquanto agente de tratamento de dados. |
| **Privacidade** | O Programa de Privacidade de **Sua Empresa** | | |
| **Segurança da Informação** | Os requisitos mínimos para garantir a Segurança da Informação se o produto ou serviço envolvem **interação tecnológica, manipulação de informação** ou **desenvolvimento de solução tecnológica**. | | |

Sempre forneça respostas **completas** e apresente **evidências** de suas afirmações, a fim de evitar Solicitações de Informações adicionais por parte do **Grupo Icatu**.

Clique nos links para ir direto à seção das avaliações

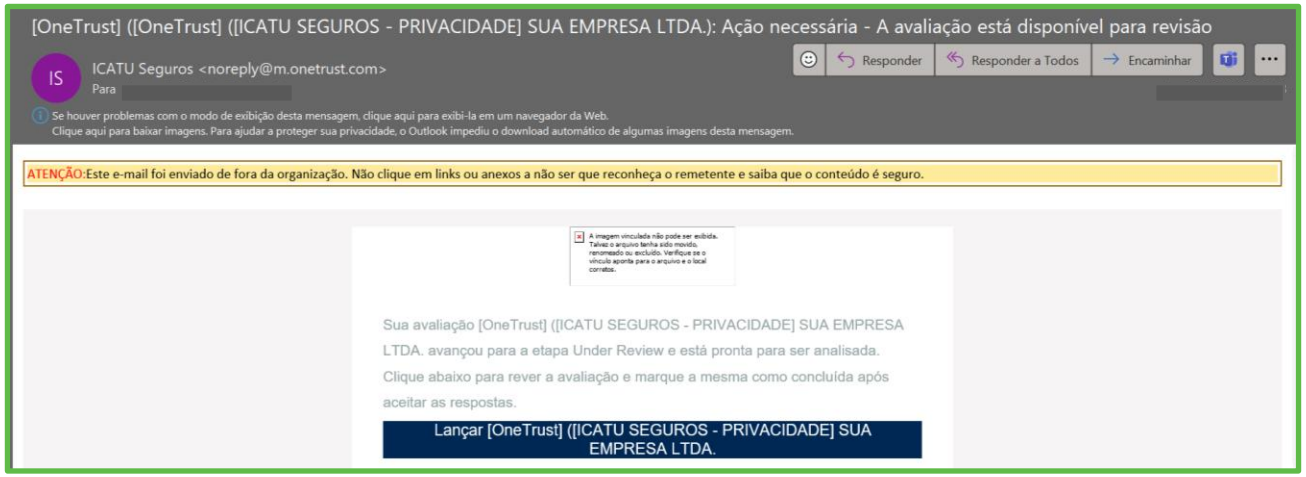
ICATU

# Recebendo o formulário

Caso **Você** tenha sido apontado/a como respondente da diligência, enviaremos o questionário ao seu endereço de email. **Você** receberá uma mensagem:

- **Do Remetente**: ICATU Seguros noreply@m.onetrust.com
- **Com o assunto no formato**: [OneTrust] ([ICATU SEGUROS – NOME DA AVALIAÇÃO] – NOME DA SUA EMPRESA): Ação necessária - A avaliação está disponível para revisão

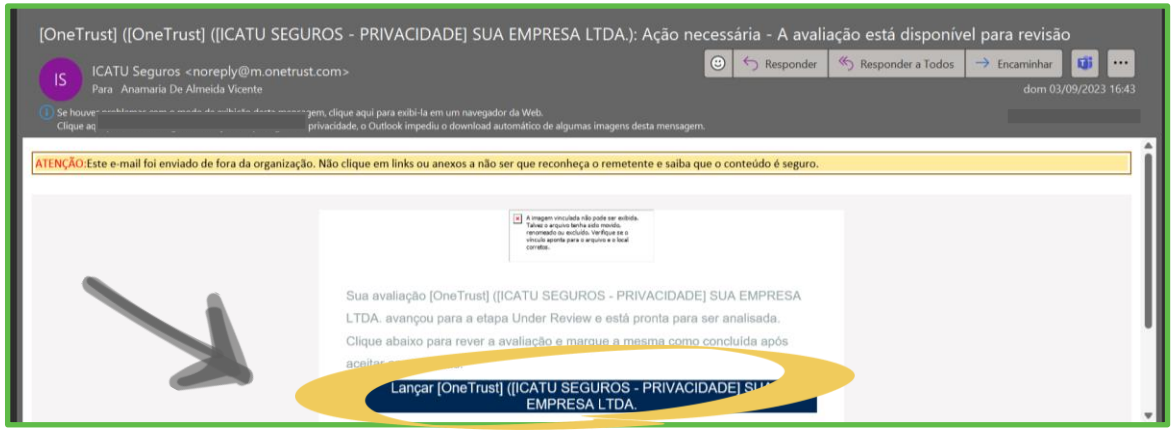
Neste exemplo, a avaliação enviada é a de Privacidade



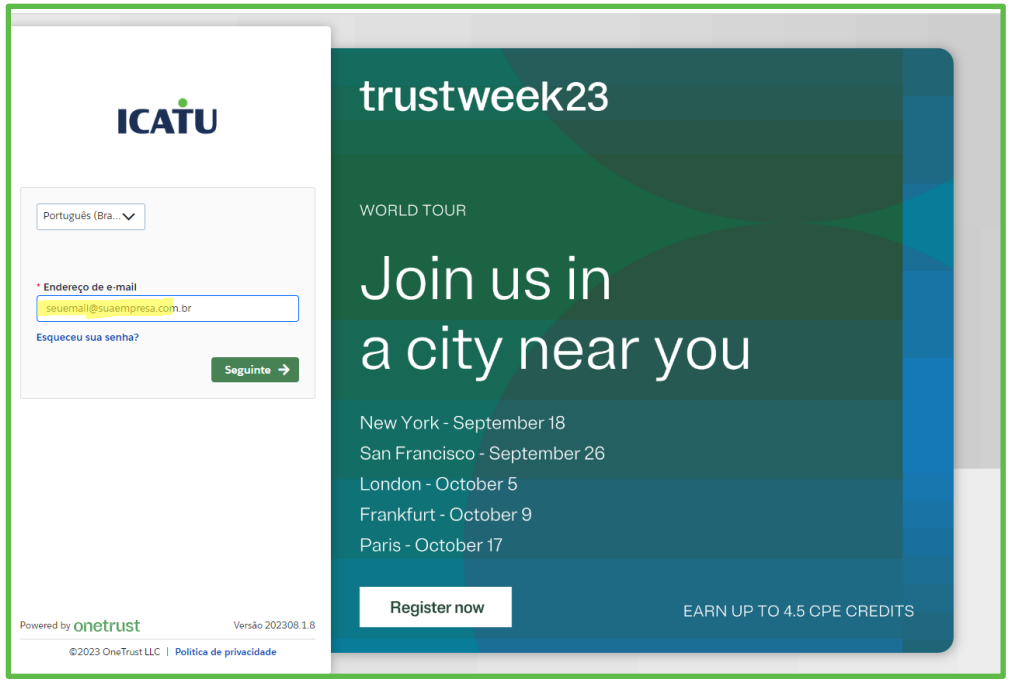

Caso não tenha recebido o e-mail na sua caixa de entrada, favor verificar sua lixeira ou caixa de *spam*.

# Acessando a plataforma

Clicando no *link* azul da mensagem, **Você** será direcionado para o ambiente OneTrust.




Se **Você** foi indicado como respondente, será redirecionado para cá. A ferramenta não exige senha de usuários cadastrados. Confira seu email e clique em "**Seguinte**".




Evite encaminhar o email a outras pessoas**.** Só pessoas cadastradas como respondente consegue acessar o formulário. Se necessário incluir outros respondentes, acione seu contato no **Grupo Icatu** e faça este pedido.

Os respondentes devem conhecer o assunto dentro de **Sua Empresa** para que a aprovação aconteça de modo ágil e produtivo. Indique como respondentes pessoas que conheçam dos temas continuidade de negócios, segurança da informação e privacidade.

A partir da data de envio, **Sua Empresa** terá até 7 (sete) dias úteis para enviar o formulário.

# Conhecendo as seções

Aqui estão todas as Solicitações de Informações, onde **Você** pode ver os novos esclarecimentos que pedimos

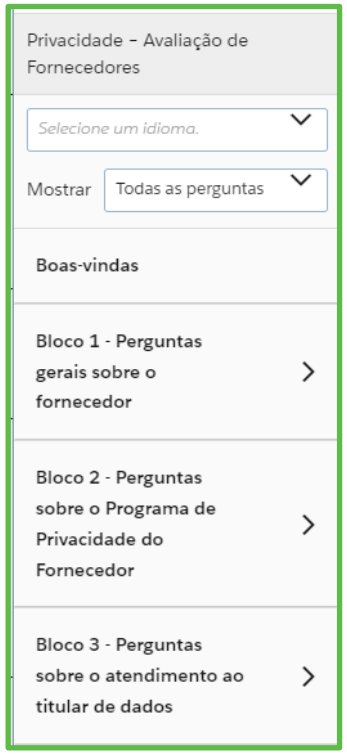
Aqui **Você** vê os anexos que incluiu

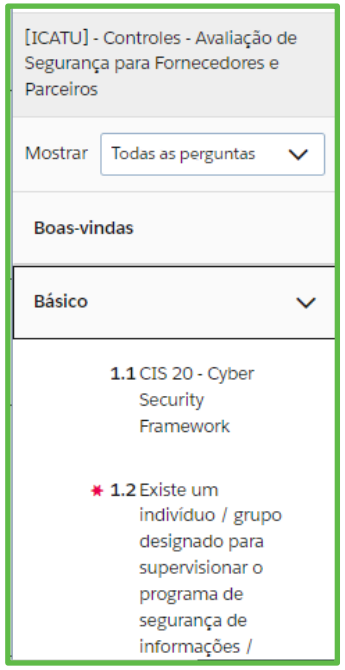

Aqui estão todos os comentários eventualmente inseridos por **Você** ou pelo **Grupo Icatu**.

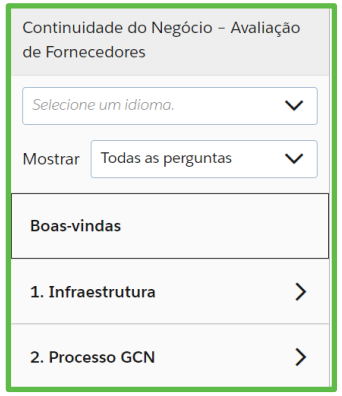
Nesta coluna à esquerda estão todos os blocos em que o questionário se divide.

**Boas-Vindas**: aqui inserimos conceitos-chave e orientações sobre como preencher o formulário

# Navegando pelos blocos

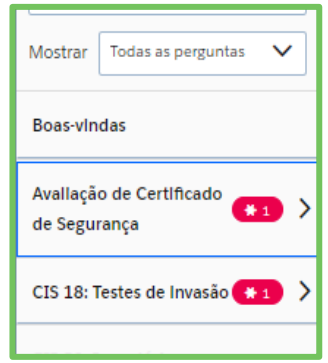


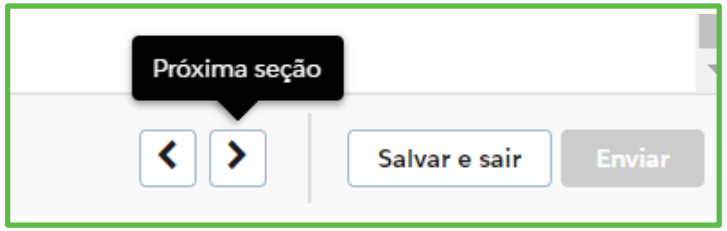

Cada diligência possui um conjunto de blocos.

Se houver uma sinalização em vermelho, como no exemplo ao lado, significa que há perguntas sem respostas. Todas as perguntas devem ser respondidas, do contrário não será possível finalizar o questionário e enviá-lo de volta ao **Grupo Icatu**.




O salvamento de cada questionário é automático, mas se preferir, **Você** pode clicar em “Salvar e Sair”, retornando ao questionário posteriormente.

Ao final de cada bloco, no rodapé de cada página, basta clicar no ícone **“>”** para avançar para o bloco seguinte.



Respondendo a diligência de

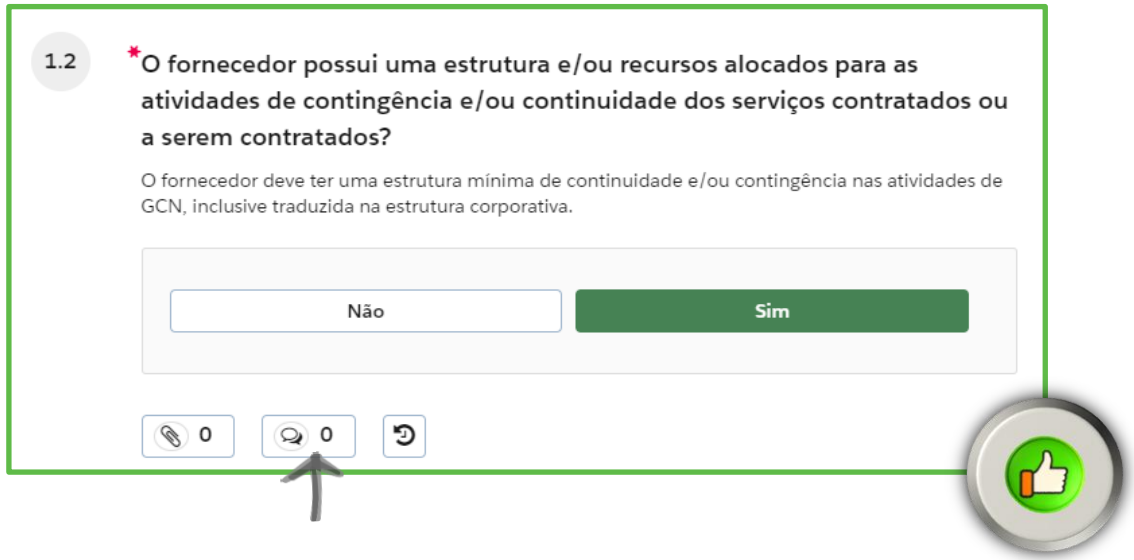
# Continuidade de Negócios

# Perguntas objetivas

Nas avaliações de Continuidade de Negócios, há dois blocos de perguntas: “Infraestrutura” e “Processo GCN”.

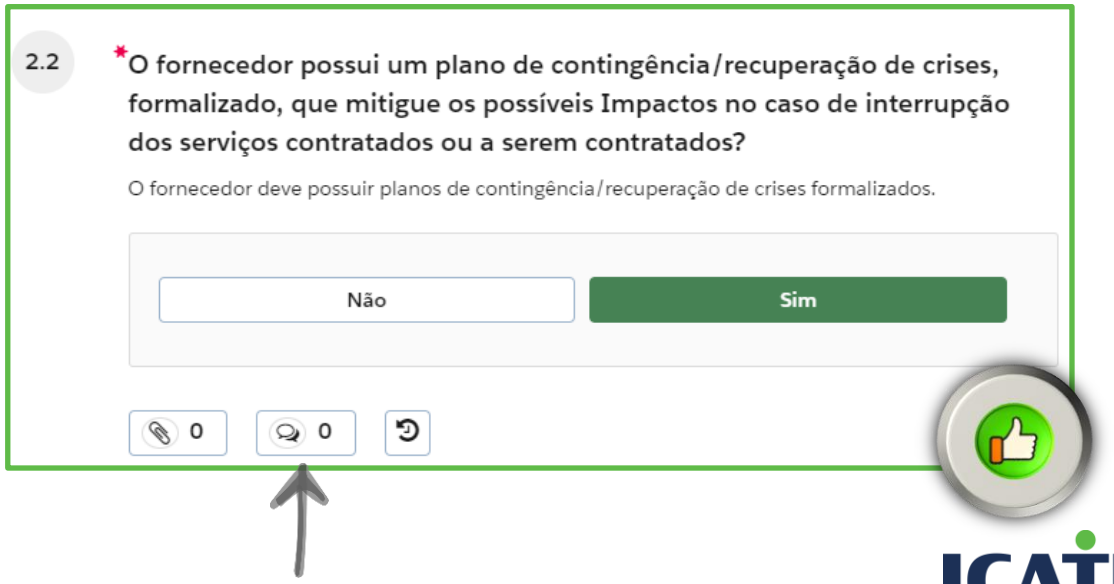
Todas as perguntas da avaliação de continuidade de negócios são objetivas. Abaixo de cada pergunta, há sempre uma explicação. Leia a explicação, juntamente com a  pergunta. Caso seja necessário, **Você** poderá inserir um comentário a respeito de sua resposta.

## Exemplo de pergunta do bloco “Infraestrutura”




Utilize o balão de comentários a seu favor, sempre que precisar fornecer justificativas sobre a maturidade e os controles de **Sua Empresa**.

## Exemplo de pergunta do bloco “Processos GCN”



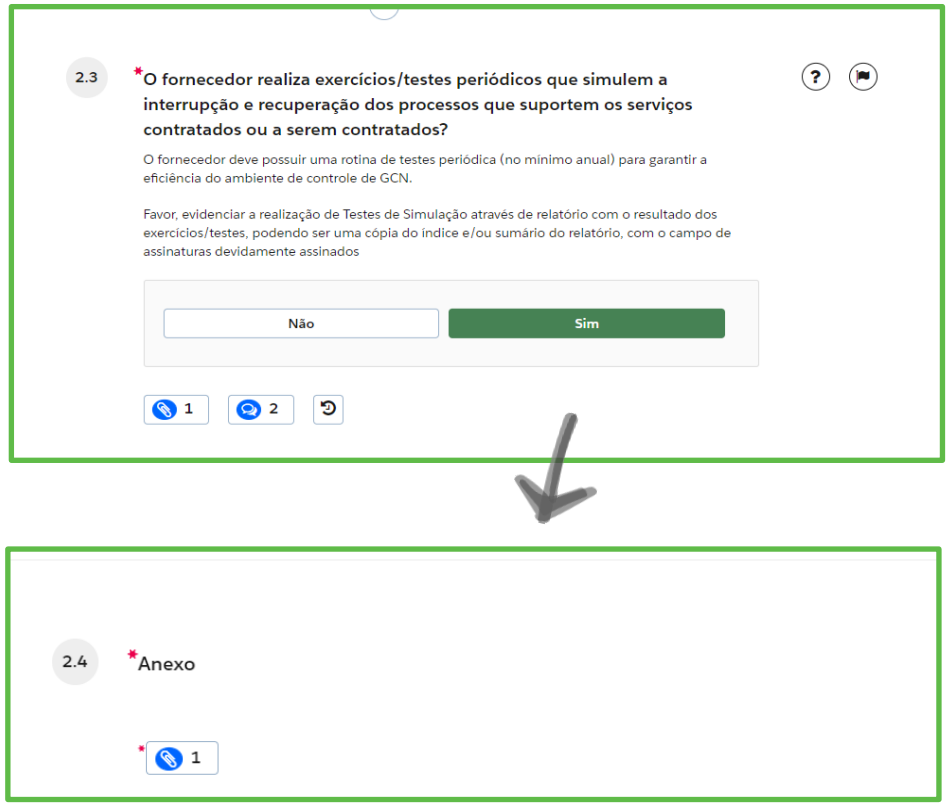

ICATU

# Anexando evidências

Há, no bloco “Processos GCN”, uma pergunta em que o **Grupo Icatu** solicita evidência de que **Sua Empresa** realiza Testes de Simulação. Se sua resposta for positiva, na pergunta seguinte, é solicitada uma evidência de sua realização. O **Grupo Icatu** solicita esta evidência a fim de garantir a eficiência do ambiente de controle de GCN.

Esta providência é essencial para que o **Grupo Icatu** avalie se **Sua Empresa** realiza exercícios periódicos que simulem a interrupção e recuperação dos processos que suportam os serviços contratados ou a serem contratados.

Pergunta sobre Teste de Simulação




Se a resposta foi “Sim” mas nenhuma evidência foi anexada, o questionário poderá ser devolvido, gerando novos questionamentos do **Grupo Icatu**.

Portanto, se **Sua Empresa** realizar testes de simulação, eles deverão ser documentados.

Caso contrário, solicitamos alterar a resposta para “Não”, a fim de evitar atrasos desnecessários na avaliação.

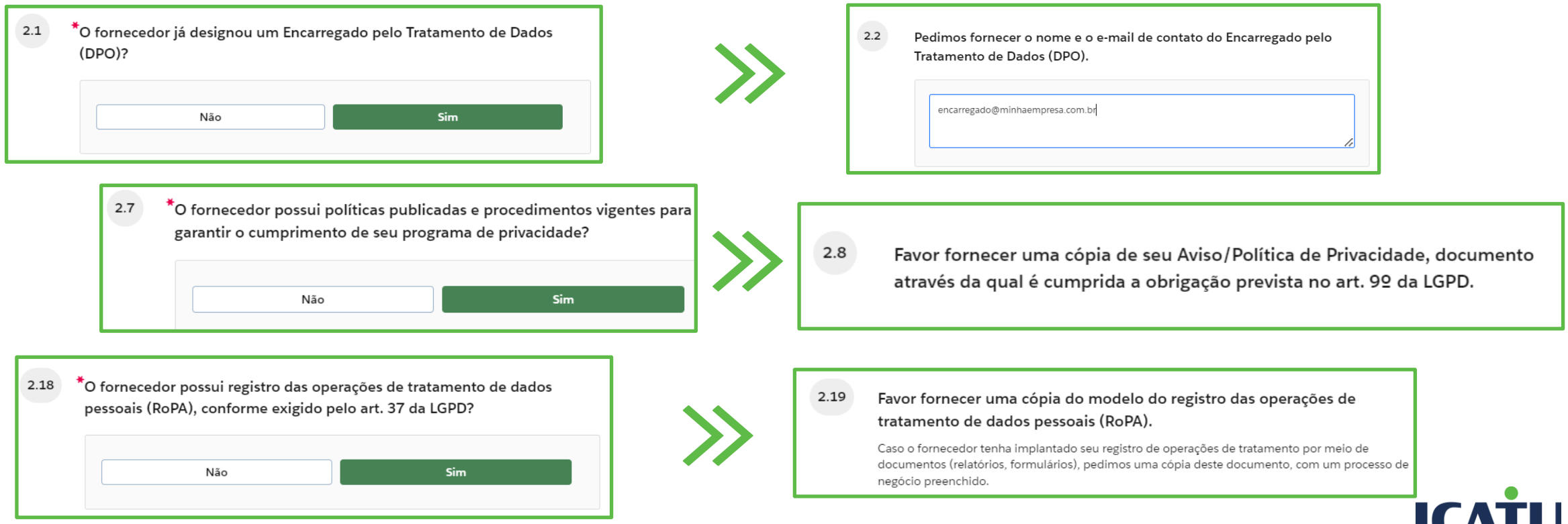
Respondendo a diligência de

# Privacidade

# Perguntas objetivas

A diligência de Privacidade contém cinco blocos de perguntas relacionadas ao Programa de Privacidade de **Sua Empresa**. Há perguntas que podem ser respondidas com “Sim” ou “Não” e outras que demandam respostas discursivas.

Quando a pergunta for respondida com “Sim”, normalmente, na pergunta seguinte, solicitamos justificar a resposta ou anexar evidências, que podem ser apresentadas nos formatos PDF, JPG, XLS, DOC, dentre outros.

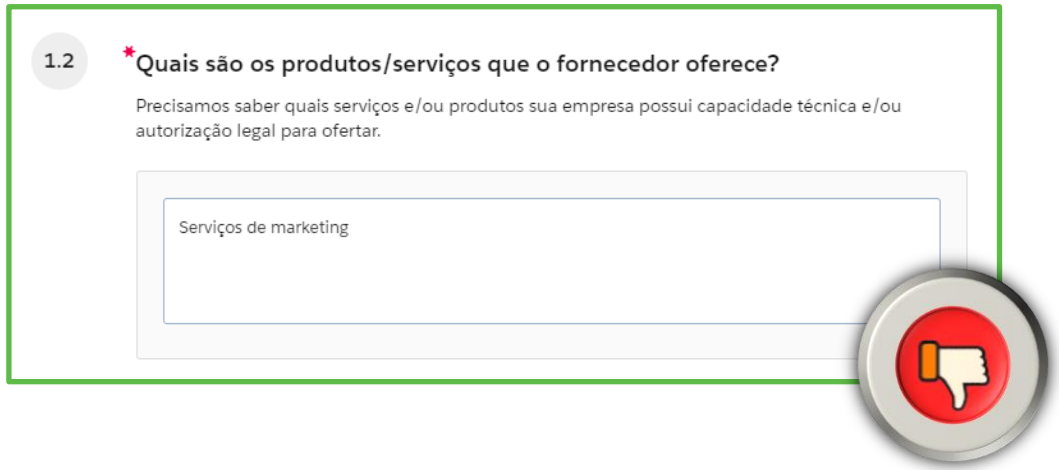



ICATU

# Perguntas discursivas

Quando a pergunta for discursiva, cabe a **Você** fornecer respostas completas e detalhadas.

Abaixo de cada pergunta, há sempre uma explicação. Leia-a juntamente com a pergunta e busque fornecer respostas completas e relacionadas ao que foi questionado. Isso ajudará o **Grupo Icatu** a avaliar **Sua Empresa** da maneira mais diligente e justa, deixando de atribuir riscos desnecessários. Veja os exemplos abaixo:





Dê respostas assertivas, que permitam ao **Grupo Icatu** entender o grau de maturidade e **Sua Empresa** e quais controles ela adota para atender a legislação. Respostas vagas e curtas farão com que o **Grupo Icatu** solicite informações adicionais, o que pode gerar atrasos na conclusão desta etapa.

Respondendo a diligência de

# Segurança da Informação

# Diligência simplificada

Há dois tipos de diligência de Segurança da Informação.

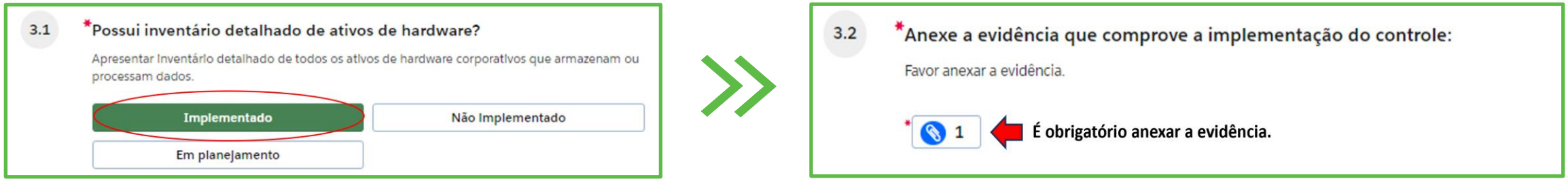
O primeiro é composto pela verificação de certificados de segurança, sendo eles **SOC2**, **ISO27001** ou **PCI,** que sejam válidos para o escopo do contrato.  Caso **Sua Empresa** possua um certificado, basta responder positivamente à pergunta 1.2, indexar a evidência na pergunta 1.3 e retornar a avaliação, conforme indicado na seção Finalizando a diligência.


Recomendamos a leitura do tópico Boas-Vindas no questionário enviado via Onetrust para esclarecer eventuais dúvidas de preenchimento.

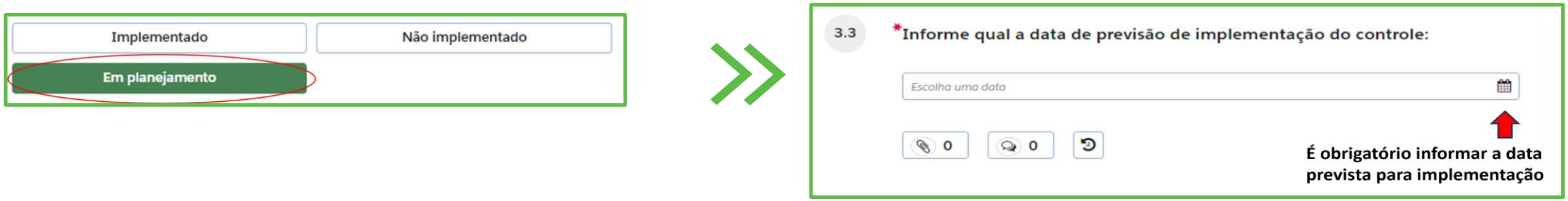
# Diligência completa

Se **Sua Empresa** não possui certificado ou se o **Grupo Icatu** identificar que o documento não é válido para o escopo, as perguntas que estavam ocultas serão ativadas, e seu preenchimento será obrigatório. Para cada pergunta, conforme apontado abaixo:

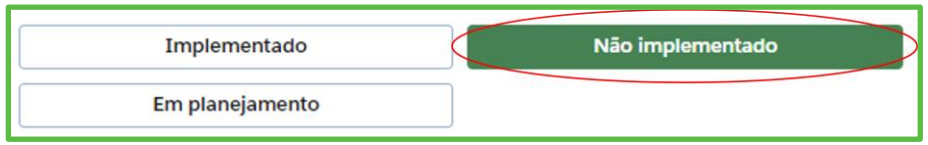
**Implementado:** ao selecionar esta opção, uma nova questão será aberta para anexar a evidência da implementação do controle




**Em planejamento:** selecionando-a, abre-se uma nova questão para informar qual a data de previsão de implementação do controle




**Não Implementado:** ao selecionar esta opção, não é necessário anexar nenhuma evidência

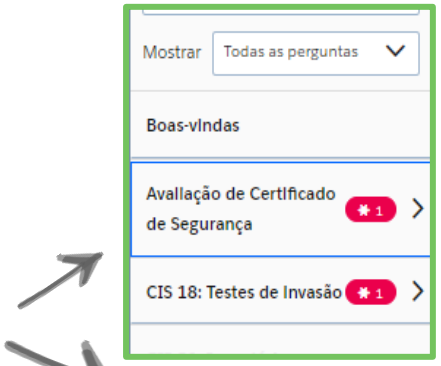


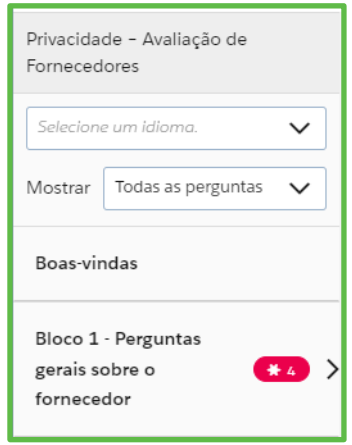
Etapas

# Finais

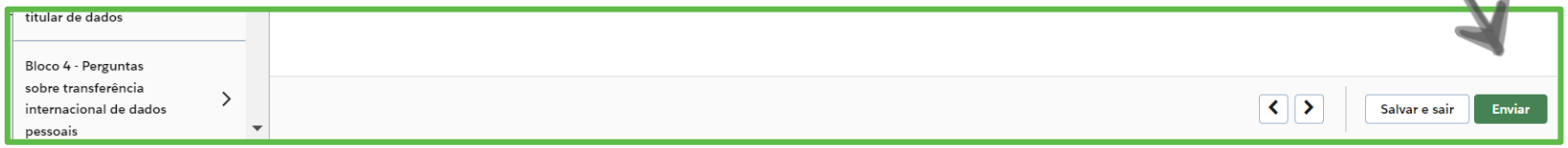
# Finalizando a diligência

Antes de finalizar, confirme se todas as perguntas possuem resposta. A sinalização "***00**" [conforme figura ao lado de cada bloco] indica que ainda há perguntas sem respostas. Se esta sinalização estiver marcada, **Você** não conseguirá enviar o questionário ao **Grupo Icatu**.




Não havendo nenhuma pergunta em aberto, será habilitado o botão verde "**Enviar**".

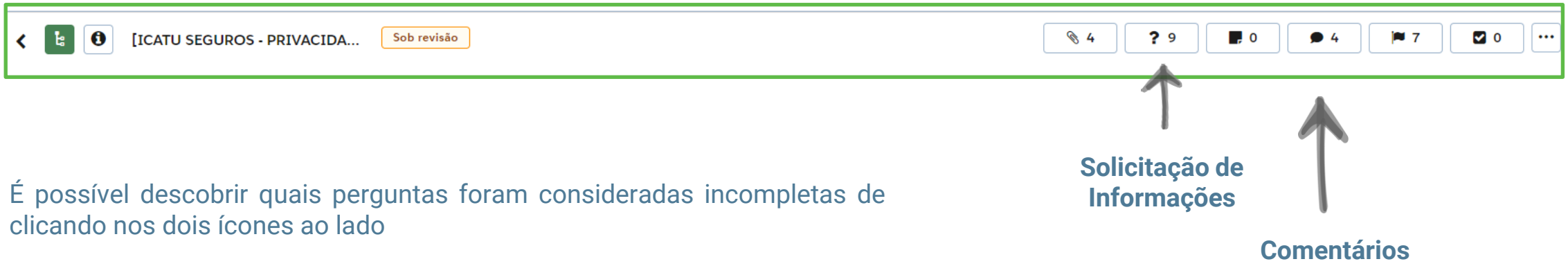



**Importante**: não basta responder a todas as perguntas, é preciso clicar em "**Enviar**". Do contrário, o **Grupo Icatu** não receberá as respostas e não poderá dar andamento à avaliação.

# Diligência devolvida

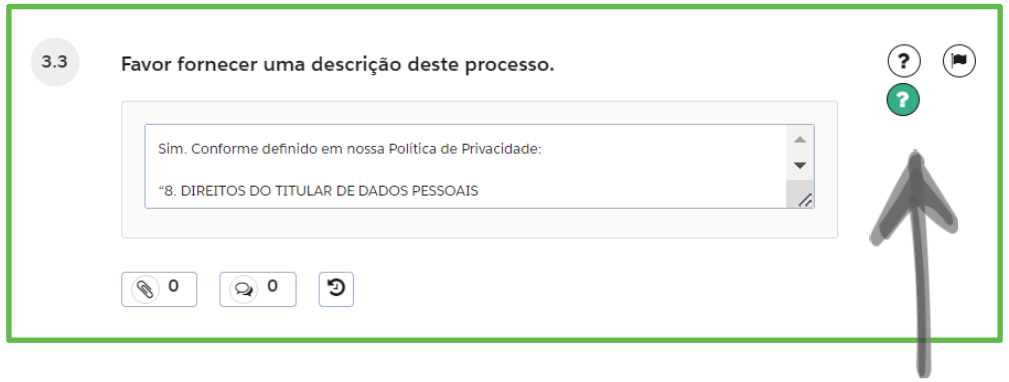
Se, depois de responder a diligência, **Você** receber outro email da OneTrust, será porque, ao avaliar as respostas, o **Grupo Icatu** pediu informações complementares ou evidências que não foram atendidas [ou foram atendidas de modo incompleto].

Será necessário repetir o procedimento das primeiras etapas: clicar no *link* do *email*, abrir o formulário, avaliar as "Solicitação de Informações" e responder às perguntas ou indexar as evidências solicitadas.




É possível descobrir quais perguntas foram consideradas incompletas de clicando nos dois ícones ao lado

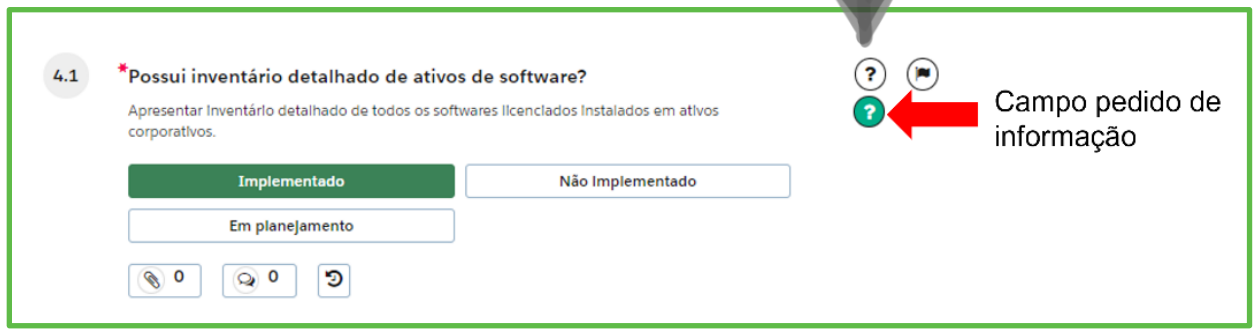
# Solicitação de informações



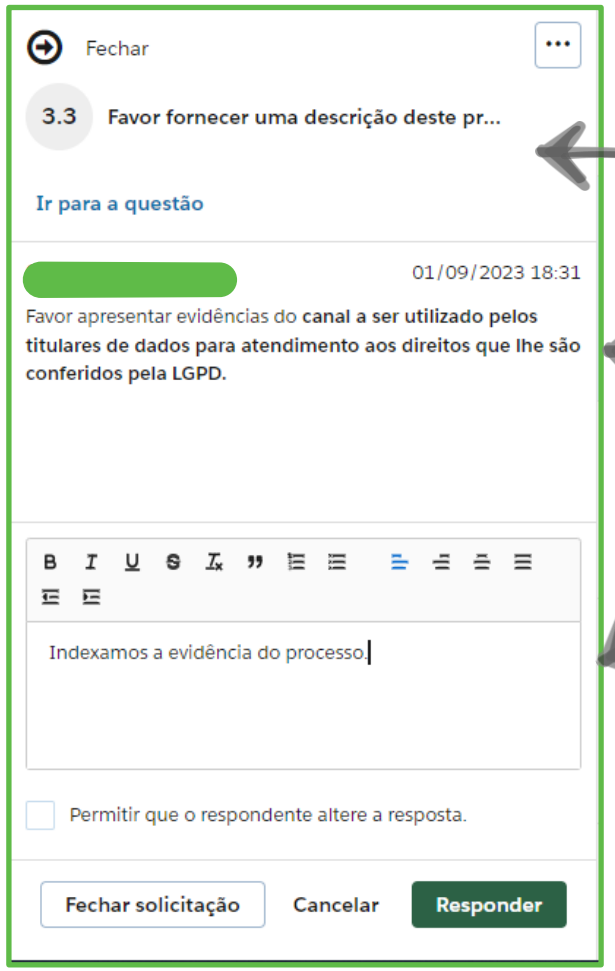

Ao abrir o formulário, é possível percorrer as perguntas que estiverem apresentando o ícone de "Solicitações de Informações", conforme a figura acima.

Essas solicitações serão inseridas no formato do ícone ao lado de cada pergunta. Basta clicar nele e a Solicitação de Informação estará numa nova janela que irá se abrir (ver próxima página).

Cada resposta será avaliada por uma das equipes do **Grupo Icatu**. Em caso de dúvidas ou pendências, a avaliação retornará para **Você** no mesmo ícone.



# Solicitação de informações




A Solicitação de Informações se abre em uma outra janela, na qual é possível:

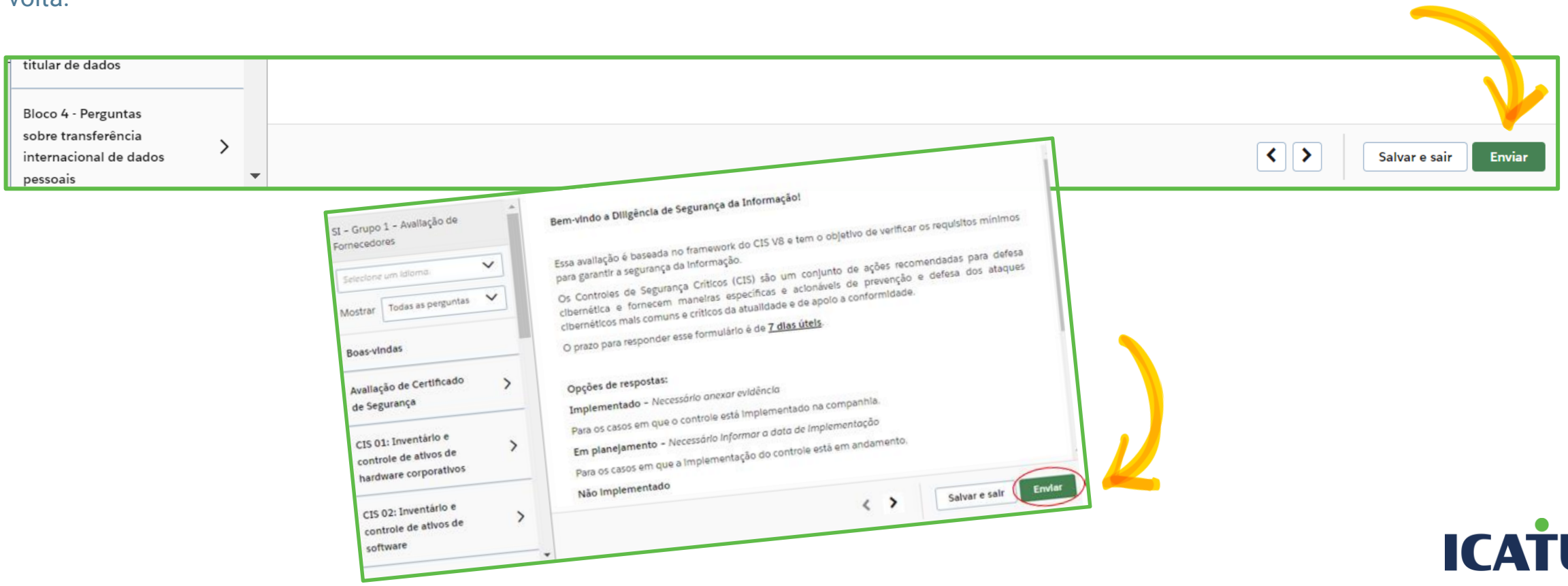
- Ver o número da pergunta à qual ela se refere (no exemplo, a pergunta 3.3 da Due Diligence de Privacidade);
- Ler a pergunta deixada pelo analista do **Grupo Icatu**;
- Responder à pergunta feita.

Responda à pergunta e clique em "**Responder**". Pedimos que além de atender ao questionamento, **Você** também informe que o fez, como no exemplo ao lado. Isso evita dúvidas por parte dos analistas do **Grupo Icatu**.

# Reenviando o formulário

Depois de responder à Solicitação de Informações, é preciso clicar no botão “**Enviar**” para que esta avaliação seja devolvida ao **Grupo Icatu**.

Pedimos que revise o questionário, garanta que ele é o mais completo possível, anexe as evidências em falta e envie o questionário de volta.



# Perguntas frequentes

**Respondi a diligência de Segurança da Informação. Preciso responder à de Privacidade e GCN?** Sim, pois as avaliações possuem objetos distintos, apesar de serem temas parecidos.

**Posso repassar a alguém da minha Empresa o email para responder a diligência?** O melhor caminho é indicar outra pessoa para responder juntamente com **Você**. Não há limites para a inclusão de respondentes.

**Meu Aviso de Privacidade está publicado no site, posso somente incluir o endereço?** Pedimos que indexe a evidência. **Você** pode anexar uma impressão da página onde o aviso, com a referência da URL onde ele está hospedado.

**Meus artefatos jurídicos (LIA, DPIA, RoPA), políticas e documentos são confidenciais, o que fazer?** Anexe uma cópia da capa do documento, do sumário e da data de publicação. Com relação aos artefatos, pode anexar um template ou layout, sem dados pessoais, ou print de seus sistemas. O intuito destas perguntas é avaliar se **Sua Empresa** adota controles e boas práticas para minimizar os riscos, e não avaliar seu teor.

Caso **Você** esteja passando por algum problema técnico e precise que o formulário seja devolvido ou que outras pessoas sejam inseridas, favor entrar em contato com a pessoa do **Grupo Icatu** responsável por sua contratação. Esta pessoa direcionará internamente seus questionamentos e iremos atender **Você** o mais rápido possível.

ICATU

ICATU

Vida. Pra toda vida.